# ¿Dónde están mis datos?

## Informe 2019

Un informe de Fundación Karisma que evalúa el compromiso que los proveedores de internet en Colombia tienen con los derechos a la libertad de expresión, intimidad y la seguridad digital de las personas.




**Autores:**
Carolina Botero
Juan Diego Castañeda

**Asistente de investigación:**
Mariana Lozano

Fundación
Karisma

Fundación Karisma hace un reconocimiento especial a otros proyectos similares que han servido como inspiración:¿Quién defiende tus datos? de R3D México, ¿Quién defiende tus datos? de TEDIC Paraguay, Quem defende seus dados? de Internet LAB Brasil, ¿Quién defiende tus datos? de Hiperderecho Perú, ¿Quién defiende tus datos? de Derechos Digitales Chile, ¿Quién defiende tus datos? de ADC Digital Argentina. ¿Quién defiende tus datos? Panamá y, a otros fuera de la región como ¿Quién defiende tus datos? de Eticas Foundation España, Who has your back? de la Electronic Frontier Foundation y Ranking Digital Rights del Open Technology Institute. También agradece a las personas de las empresas evaluadas que se reunieron con el equipo de trabajo de la Fundación y que se han estado esforzado en mejorar los resultados de este ejercicio.

**Autores:**
Carolina Botero y Juan Diego Castañeda

**Investigación:**
Mariana Lozano

**Revisión:**
Alejandra Martínez

**Coordinación Editorial:**
Diego Mora y Alejandra Martínez

**Diagramación y diseño gráfico:**
Daniela Moreno

Bogotá, Colombia
Marzo de 2020

# Tabla de contenidos

# Sobre el informe

¿Dónde están mis datos? busca explicar cómo responden las empresas proveedoras de servicios de internet a sus obligaciones en materia de derechos humanos. Su primera versión fue publicada en el año 2016; desde entonces Fundación Karisma repite este ejercicio cada año para que las personas usuarias de servicios de internet en el país tengan más información a la hora de escoger a su proveedor.

Los operadores de telefonía celular e internet son muy importantes para el ejercicio de los derechos humanos. Como intermediarios, conocen, por ejemplo, lo que hacemos a través de sus servicios, las páginas que visitamos y las personas a quienes llamamos, por cuánto tiempo, e incluso aproximadamente desde qué lugar. Esta información es utilizada por los operadores para mejorar sus portafolios o diseñar ofertas, pero también, en términos legales es requerida por algunas autoridades públicas. Además, las redes de comunicaciones son un punto de interceptación al que pueden acceder autoridades como la Fiscalía para investigar hechos delictivos.

Como ya es tradición, ¿Dónde están mis datos? analiza especialmente la forma cómo estas empresas se aproximan a la protección de la libertad de expresión e intimidad de las personas que usan sus servicios, y más recientemente, algunas de sus prácticas en seguridad digital. Es importante tener presente que la evaluación indaga solo sobre las políticas e información que publican las empresas. No evaluamos lo que efectivamente hacen sino lo que dicen hacer. El propósito del informe no es analizar si cumplen con la ley, es proponer estándares exigentes, incluso más allá de la ley, para proteger los derechos humanos[1].

Cuando iniciamos con este ejercicio en el año 2015, las políticas de protección de datos de las empresas eran, en general, copias de la ley, en formatos que no permitían ni buscar palabras para navegar su contenido. Después de cinco años, las empresas han ajustado sus políticas para dar más información a las personas usuarias. Algo similar ha sucedido en relación con los bloqueos de contenidos en Internet. Hoy sabemos más sobre el marco legal de esta situación y sobre cómo lo hacen las empresas.

En 2019 se analizaron las mismas empresas de ediciones anteriores -aunque en este ejercicio desapareció Telebucaramanga y por tanto no fue objeto de evaluación- y, si bien, en líneas generales se mantuvieron los mismos criterios de evaluación, podemos mencionar algunos ajustes que apuntan a sus mayores niveles de exigencia:

---

*1. La metodología usada para esta evaluación puede consultarse en* [*"Metodología 2019, ¿Dónde están mis datos?*]

1. En relación con los informes de transparencia para la evaluación ya no basta con publicar la información que consideramos debe tener un informe de esta naturaleza. Para 2019 se evaluó que expresamente incluyeran información sobre las solicitudes de datos del suscriptor, sobre los bloqueos de URL y sobre las interceptaciones a las comunicaciones ordenadas por las autoridades.

2. En relación con las políticas de protección de datos tampoco es suficiente que las empresas las hagan públicas y expliquen cómo lo hacen. Para 2019 se evalúan detalles concretos del contenido de esas políticas, se evalúa que indique cuáles son los datos que recoge, lo usos que hace y si indica que hay terceros que acceden a esos datos.

3. Sobre el procedimiento para la entrega de información a autoridades del sector público, se considera la importancia de que este incorpore mecanismos garantistas de derechos humanos.

4. Dentro del grupo de temas que se analizan en materia de intimidad en 2019 se estableció un criterio independiente sobre la información que las empresas comparten con otros privados.

5. En 2019 ya no basta con informar sobre la obligación de bloqueos. Se evalúa si la empresa lista los diferentes casos que el marco legal colombiano contempla sobre este tema.

6. En relación con el procedimiento para bloqueos se busca ir más allá de las causales legales e incorporar los bloqueos derivados de los contratos suscritos por las personas usuarias.

De las seis empresas evaluadas, el cuadro general muestra que **Movistar tiene la mejor calificación** seguida de cerca por Claro y Tigo. En el siguiente nivel están ETB y DirecTV, **en el último lugar se encuentra EMCALI.** En los primeros años de ¿Dónde están mis datos? la empresa nacional y semi privada ETB dió una importante lección de adaptación y apuesta por los derechos humanos de las personas usuarias, en su momento asumió liderazgo en los cambios. Sin embargo, para esta edición ha quedado relegada por las grandes empresas que son las que ahora están avanzando en estas agendas. Desde que evaluamos EMCali ha estado atrás en esta evaluación. Con esta empresa no hemos podido tener un acercamiento para explicar el alcance y beneficios de esta herramienta para la empresa y para las personas usuarias de sus servicios.

A cinco años de haber iniciado este proyecto es muy satisfactorio para Karisma ver los avances que han tenido las empresas en los temas que se evalúan. El más importante de todos tiene que ver con que cuatro empresas, que juntas tienen la mayor parte del mercado en el país, publican periódicamente información del estilo que es usual a nivel internacional para un informe de transparencia. Dos de ellas -Claro y Movistar- obtienen el máximo puntaje. Es decir, hoy en día contamos con información sobre qué autoridades piden nuestros datos y cuántas veces lo hacen; inclusive, algunas empresas nos dan más datos.

Algo similar ha sucedido en relación con los bloqueos de contenidos en Internet, hoy sabemos más sobre el marco legal de esta situación y sobre cómo lo hacen las empresas, también en este caso a las tres empresas punteras Movistar, Claro y Tigo, se une ETB.

Otro éxito que podemos establecer en la línea de tiempo del informe es que para 2019 todas las seis empresas han implementado https en sus páginas web. Ahora bien, en casi todos los demás aspectos hay muchas oportunidades de mejora.

Para las personas en general y para las organizaciones de la sociedad civil, es útil contar con informes de transparencia que sean comparables. Los datos que proveen estos informes permiten controlar los poderes del Estado en relación con los derechos de las personas. Las empresas pueden y deben trabajar para estandarizar sus informes y facilitar estos procesos generando un valor agregado para que las personas puedan entender mejor qué sucede con sus datos en un entorno digital. La protección de datos personales es un tema vigente mundialmente como pocos.

En 2019 Algunos cambios hicieron más estrictos los criterios de evaluación sobre el eje de intimidad, afectando la calificación de todas las empresas en este año, en comparación con lo sucedido en 2018. Aún así, podemos afirmar que frente al 2015 hoy en día las políticas de protección de datos son herramientas efectivas para que las personas interesadas puedan informarse mejor. Antes esas políticas, en general, eran copias de la ley en formatos que no permitían siquiera buscar palabras para navegar su contenido.

Karisma cree que la forma de apoyar la protección de la intimidad está relacionada con la posibilidad de que los operadores ofrezcan más información a las personas que usan sus servicios. Por tanto, esta vez la evaluación se hizo más estricta y tiene que ver con el tipo de datos y los plazos durante los cuales los conservan, además de los criterios y procedimientos para hacerlo. El análisis va más allá de cuando esto lo hacen las autoridades públicas, también se trata de explicar sus políticas para compartir la información con otros privados. Aunque en este tema todas las empresas tienen vacíos,Tigo es la que mejor se ranquea, DirecTV, Movistar y Claro le siguen. Vale la pena resaltar que DirecTV es la única que parece ofrecer avisar -notificar- a las personas cuando las autoridades piden información sobre ellas. Ahora bien, el problema es que no es un compromiso sino una “posibilidad”. Finalmente, Claro es la única que hace una descripción del procedimiento que aplica para la entrega de datos al sector público.

En materia de libertad de expresión las empresas proveedoras de internet en el país tienen un compromiso con la neutralidad de la red que las obliga a no interferir en la navegación de las personas que usan sus servicios. Dado que el marco jurídico les impone obligaciones de bloqueo, en Karisma creemos que una forma de proteger la libertad de expresión es dando transparencia a esta obligación, es decir, entregando información sobre la forma como estos bloqueos se hacen. La información que están entregando estas empresas sobre los bloqueos vinculados especialmente con contenido de explotación sexual de menores y sobre comportamientos no permitidos ha mejorado sustancialmente. Movistar y Tigo puntean en este criterio, seguidos de Claro y ETB.

Desde el contexto de seguridad digital Movistar es la que más información ofrece sobre su forma de enfrentar incidentes de seguridad. Además indica expresamente que reporta incidentes de seguridad a la autoridad de protección de datos. En este punto todavía hay mucho para mejorar, por ejemplo, las buenas prácticas sugieren informar al Colcert -organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa- y también a las personas afectadas en un tiempo razonable.

Después de cinco años de esta evaluación nuestro reconocimiento está con las empresas que han entendido el valor que este ejercicio tiene en sociedades democráticas por la forma como empodera a las personas que usan sus servicios y les permite entender y ejercer mejor esos derechos.

El informe que presentamos este año tiene una estructura diferente y trae unos casos concretos de resaltar que esperamos inspiren a nuevos avances en 2020.

# Principales hallazgos

| | Claro | EMCALI | movistar | tigo | etb | DIRECTV |
|---|---|---|---|---|---|---|
| COMPROMISOS POLÍTICOS | Cumple parcialmente | Cumple de forma insuficiente | Bonificación por lenguaje incluyente en política de genero | Cumple de forma insuficiente | Cumple parcialmente | Cumple de forma insuficiente |
| INTIMIDAD | Cumple parcialmente | No cumple | Cumple satisfactoriamente | Cumple satisfactoriamente | No cumple | Cumple parcialmente |
| LIBERTAD DE EXPRESIÓN | Cumple satisfactoriamente | No cumple | Cumple todos los parametros | Cumple todos los parametros | Cumple satisfactoriamente | No cumple |
| SEGURIDAD DIGITAL | Cumple parcialmente | Cumple parcialmente | Cumple todos los parametros | Cumple parcialmente | Cumple parcialmente | Cumple parcialmente |

- Cumple todos los parametros
- Cumple satisfactoriamente
- Cumple de forma insuficiente
- Bonificación por lenguaje incluyente en política de genero
- Cumple parcialmente
- No cumple

| | Claro | EMCALI | movistar | tigo | etb | DIRECTV |
|---|---|---|---|---|---|---|
| **1. COMPROMISOS POLÍTICOS** | | | | | | |
| 1.1 Política de género | | — | | | | |
| 1.2. Política de accesibilidad | — | | | — | — | — |
| 1.3. Informes de transparencia | | — | | — | | — |
| **2. INTIMIDAD** | | — | | | — | |
| 2.1. Políticas de protección de datos | | | | | | |
| 2.2. Informa la obligación legal de retención de datos | | — | | | | |
| 2.3. Informa las razones para responder a solicitudes de información del sector público | | — | | | — | — |
| 2.4. Procedimiento de entrega de datos al sector público | | — | | | — | — |
| 2.5. Notifica a las personas sobre la entrega de datos a entidades públicas | — | — | — | — | — | |
| 2.6 Criterios para el tratamiento de datos en relación con aliados comerciales | — | — | — | | — | |
| **3. LIBERTAD DE EXPRESIÓN** | | — | | | | — |
| 3.1. Informa sobre la obligación legal de bloqueo | | | | | | |
| 3.2 Procedimientos de bloqueo (incluye obligación contractual) | | — | | | | — |
| 3.3. Guía sobre comportamientos no permitidos | | — | | | | — |
| **4. SEGURIDAD DIGITAL** | | | | | | |
| 4.1. Informa de fuga de datos personales y acciones de mitigación | — | — | | — | — | — |
| 4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web | | | | | | |

Las evaluaciones de ¿Dónde están mis datos? 2019 se llevaron a cabo durante dos períodos separados. Entre mayo y septiembre de 2019, realizamos una evaluación preliminar que compartimos con las empresas evaluadas que se interesaron en conocer sus resultados. Después de esta primera experiencia, llevamos a cabo una evaluación final en septiembre, que ajustamos tomando en cuenta los cambios recientes que las empresas nos mostraron o implementaron previo a este período. En términos generales, las empresas obtuvieron un puntaje menor en 2019 pero esto se explica porque la evaluación se hizo más estricta, no porque se hubiera deteriorado la posición de la empresa.

En esta oportunidad, presentaremos los **principales hallazgos de 2019** a partir de una serie de preguntas que faciliten la lectura de los resultados, seguidas de recomendaciones para las empresas:

## ¿Cómo informan sobre solicitudes de datos personales, interceptación y bloqueos por parte del Estado?

En nuestra relación con los operadores nos jugamos nuestros derechos a la intimidad, protección de datos y libertad de expresión, entre otros. Por eso es importante que estas empresas tengan un mecanismo para informarnos sobre cómo usan nuestros datos, a qué autoridades o empresas los entregan y en qué condiciones.

Existen diferentes mecanismos que los operadores pueden utilizar para informar a las personas usuarias sobre sus prácticas con respecto a los datos que recolectan. En ¿Dónde están mis datos? nos interesamos por dos: informes independientes, como los de transparencia, y documentos que requiere la ley, como las políticas de protección de datos.  Acá nos preguntamos sobre la forma como los operadores informan de sus compromisos y prácticas en relación con los datos de las personas, los datos que nos dan sobre lo que pasó en un período de tiempo.

Dada la  importancia de esta información para decidir a qué operador entregar los datos, nos fijamos en si estos documentos son públicos, claros y accesibles.



## ¿Qué dice la ley?

La ley colombiana no obliga a los operadores a presentar informes de transparencia o informes periódicos sobre los requerimientos que las autoridades hacen de los datos de sus clientes. Sí tienen obligación de entregar información pero sobre los planes de internet y telefonía celular o las prácticas de gestión de tráfico. Sin embargo, dar información sobre lo que sucede con los datos que recolectan se ha convertido en una buena práctica internacional especialmente entre las empresas del sector TIC.

## ¿Cómo informan los operadores?

Las empresas que ofrecen internet en Colombia presentan informes anuales muy variados. Desde hace un par de años, publican información que se relaciona con la transparencia en su compromiso de derechos humanos con sus clientes.

La mayoría de estas empresas mezclan información financiera con información sobre cómo protegen la privacidad y la libertad de expresión de de las personas usuarias, lo que puede generar confusión.

Varias de las empresas más importantes que ofrecen internet en el país son multinacionales, por tanto la información de Colombia aparece frecuentemente en sus informes internacionales.Sin embargo, en línea con los comentarios que hicimos en el pasado, los operadores han incorporado la información local en las publicaciones para nuestro país. Esto todavía no sucede con todas las empresas. DirecTV por ejemplo, ofrece tan solo información sobre las solicitudes de datos que las autoridades colombianas hacen a la empresa matriz (AT&T), esto da información interesante sobre transferencia de datos entre países, pero no sustituye información sobre lo que sucede con la gestión de los datos personales de los clientes de DirecTV.

Aunque, en general, los informes han mejorado año a año, todavía no son informes con datos comparables. Con el propósito de estandarizar las cifras para que la transparencia de los operadores sirva como mecanismo de control, en esta sección empezamos a evaluar la presencia de elementos específicos como los relacionados con solicitud de datos del suscriptor, bloqueos de URL e interceptación de líneas telefónicas.

**Claro** y **Movistar** cumplieron con todos los requisitos. Por su parte, **ETB** publica información en la misma línea del año anterior pero, en relación con los tres elementos nuevos del informe de transparencia, no hay información clara ni fácil de acceder. En su informe tiene detalles en relación con los requerimientos de información de entidades públicas. ETB sigue dando información sobre el mecanismo legal para interceptación de comunicaciones. El último informe de gestión y de transparencia que tiene **Tigo** tiene información de 2017 y no incluye información sobre el bloqueo de URL, por tanto no se da calificación este año. Finalmente, **DirecTV** y **EMCALI** no tienen información en esta parte y no hay una mejora frente a la evaluación del año pasado. La casa matriz de DirecTV tiene un informe de transparencia mundial donde informa el número de solicitudes de información que recibe la multinacional. En este caso no hay información específica para Colombia.

## Recomendaciones

- Para garantizar los derechos a la intimidad y libertad de expresión de los usuarios, los operadores en Colombia deben mejorar la buena práctica de publicar informes de transparencia; en un documento unificado, que tenga como propósito estandarizar la información a través del trabajo conjunto de su gremio.

- En 2019 revisamos los criterios generales. Para 2020, los operadores pueden dar más detalles sobre cada uno de los puntos sobre los que entregan información. Por ejemplo, se debe especificar qué entienden por datos del suscriptor, indicar los motivos de solicitud de datos por parte de entidades públicas y cuál fue la decisión del operador, discriminar entre bloqueos temporales y permanentes de URL y los bloqueos equivocados y sus motivos.

- ETB puede informar sobre las solicitudes de interceptación de comunicaciones que reciba tanto para fijos como para móviles.

- DirecTV podría hacer un informe específico para Colombia en donde recoja como mínimo la información que ya otros operadores publican en sus distintos informes.

Los datos sobre las órdenes de interceptaciones telefónicas que reciban de la Fiscalía es uno de los asuntos que esperamos que las empresas que dan acceso a internet reporten en sus informes de transparencia. Consideramos que este ejercicio ayuda a las personas a transparentar la actividad de la autoridad dado que en Colombia existen pocas instancias para hacer control de las actividades de vigilancia de las comunicaciones.

La transparencia incluye saber que en Colombia las autoridades tienen acceso directo para hacer las interceptaciones, sin intervención de la empresa que tiene las redes. En 2018, Claro incluyó en su informe de gestión que solo podía dar datos de interceptaciones de comunicaciones a líneas fijas porque en las celulares esta acción se realiza directamente, sin la mencionada mediación. Las empresas que ofrecen el acceso a internet ya no pueden dar cuenta del número de interceptaciones que se realizan en sus redes celulares. La transparencia en este caso supone que estas empresas nos dejen esta situación clara. El efecto del acceso directo que tienen las autoridades a las redes celulares del país es, entre otros, que el público tiene menos información para hacer control de esta actividad.

En 2019 Movistar y Tigo se unieron a Claro para indicar que en el país hay acceso directo de las autoridades a las redes celulares.

## ¿Cómo informan sobre los procesos de entrega de datos al sector público?

Los operadores de telefonía tienen distintos datos de las personas. Desde datos de identificación como nombre, cédula y dirección, hasta datos que generan los celulares sobre su ubicación geográfica y redes de contactos. En esta sección preguntamos cómo informan los operadores sobre dos procedimientos específicos. Primero, sobre la retención de datos y segundo, el procedimiento que usan para entregar datos personales a las autoridades públicas.

### Retención de datos

Un celular produce automáticamente muchos datos que pueden revelar información importante de las personas. Por ejemplo, se puede conocer la ubicación del celular casi en tiempo real, conocer qué otros celulares se conectan en esos mismos lugares. El análisis de todos estos datos podría servir para descubrir hábitos de las personas.

#### ¿Qué dice la ley?

Cuando hablamos de retención de datos nos referimos específicamente a la obligación que tienen los operadores de conservar y entregar a las autoridades de inteligencia y a la Fiscalía General, la información que producen los celulares en relación con el servicio de telecomunicaciones.

Los operadores deben colaborar con la Fiscalía General de la Nación para entregar, en el marco de una investigación penal, los siguientes datos[2]:

1. Los datos del suscriptor, tales como identidad, dirección de facturación y tipo de conexión. Además deben conservarla por cinco años.

2. Información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuya a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación. Deben suministrarla en tiempo real en caso de que se requiera.

La ley de Inteligencia y contrainteligencia obliga a los operadores a entregar a agencias de inteligencia[3].

1. El historial de comunicaciones de los abonados telefónicos vinculados, es decir, de las personas que contratan sus servicios.

2. Los datos técnicos de identificación de los suscriptores sobre los que recae la operación.

3. La localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización.

Sin embargo, de toda la información que pueden producir los operadores sobre la actividad de los celulares, no está claro exactamente qué entregan a las autoridades de investigación penal e inteligencia cuando deben cumplir con estas normas. Por eso, en esta pregunta nos preocupamos por cómo informan:

1. A las personas usuarias sobre la existencia de esta obligación.
2. Sobre qué datos retienen en concreto.
3. Sobre el tiempo por el cual los retienen.

Además de las normas de retención de datos que acabamos de exponer, la Fiscalía puede realizar la "búsqueda selectiva en bases de datos"[4]y las autoridades, en general, pueden solicitar datos personales sin autorización del titular, siempre que sea en ejercicio de sus funciones[5]. No está claro cómo funcionan en la práctica cada una de estas facultades ni cómo se relacionan entre ellas.

*2. Decreto 1704 de 2012, artículo 4.*
*3. Ley 1621 de 2013, artículo 44.*
*4. Ley 906 de 2004. Código de Procedimiento Penal. Artículo 244.*
*5. Ley 1581 de 2012. Artículos 10 y 13.*

## ¿Qué informan las empresas que dan acceso a internet?

En este punto no revisamos el resultado de la actividad de retención de datos. Por ejemplo, el tipo de datos de las personas usuarias que entregaron a la Fiscalía. Acá revisamos la forma como los operadores informan que desarrollan su obligación, cuáles son los datos que retienen y por cuánto tiempo. Los operadores, basados en el cumplimiento de la ley, publican que deben retener los datos de las personas usuarias y varios ya hacen referencia a las normas que se aplican. Sobre los datos que conservan para entregar a las autoridades en investigaciones penal o de inteligencia o el tiempo que dura la retención, los operadores no siempre dan detalles.

**Tigo**, **Movistar** y **Claro** informan sobre la existencia de la obligación legal pero, tan solo Movistar presenta información del tipo de datos que retiene.

En cuanto al tiempo durante el cual guardan los datos, Claro habla de 10 años, en tanto que Tigo, DirecTV y Movistar tiene cláusulas muy amplias que dicen conservar los datos por el tiempo que dure la relación contractual e incluso más.

ETB, solamente pública que está obligada a retener datos y no informa sobre el tiempo ni tampoco sobre el tipo de datos que retiene.

## Recomendaciones

Para Karisma, es importante que las empresas que dan el acceso a internet en Colombia informen expresamente las normas que los obligan a retener datos personales de sus clientes, por cuánto tiempo conservan la información, cuáles son los datos que guardan y qué hacen con ellos. Debido a que no todas las personas usuarias tienen conocimiento de que estas acciones se realizan por obligación legal. Tampoco saben qué hacen las empresas con esos datos durante el tiempo que los deben conservar. La mejor manera de solucionar estos vacíos es aumentando la información que ofrecen. Concretamente, deberían ampliar la información sobre:

- El tipo de datos en relación con la información que revela sobre las personas usuarias, por ejemplo, Movistar explica cuáles son los metadatos que las autoridades solicitan en sus requerimientos.
- La duración de la retención según el criterio que usen, o el tipo de dato retenido. Como mínimo, es económicamente imposible guardar los datos de todas las personas suscriptoras por tiempo indefinido, por tanto todas las empresas de este tipo tienen que tener algún criterio para definir qué conservan y por cuánto tiempo.



**ETB** y **EMCALI** son las que menos calificación reciben en este caso. Para mejorar esta evaluación podrían dar detalles sobre el tipo de datos que guardan y el tiempo por el que los retienen.

## Solicitudes por parte de entidades públicas

Los operadores no solo reciben solicitudes de la Fiscalía, legalmente otras autoridades tienen facultades legales para hacer este tipo de solicitudes. En este punto queremos entender cómo informan los operadores sobre la entrega de datos personales a entidades públicas y los procedimientos que usan para estos casos.

### ¿Qué dice la ley?

La Ley de Protección de Datos permite la entrega de datos personales a entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial sin autorización de la persona titular de los datos[6]. Las autoridades que reciben la información deben guardarla en reserva, usarla sólo para los fines para los cuales la recibieron, deben informar a los titulares del dato sobre el uso que le dan y tomar medidas de seguridad para protegerla[7].

### ¿Qué informan los operadores?

**Movistar**

Publica el procedimiento para Colombia. En su informe anual de transparencia señala que en cada país en que opera la multinacional crea un procedimiento interno que se ajusta a las normas locales y responde a principios de "Confidencialidad, Exhaustividad, Fundamentación, Respuesta Diligente y Seguridad". Adicionalmente, incluye la lista de las autoridades que tienen competencia en Colombia para hacer requerimientos de información.

Movistar indica que en la recepción de las peticiones participan áreas con competencias legales e interlocutores fijos mediante ventanilla única para atender a las autoridades competentes. Afirman rechazar cualquier petición que no viene por este conducto reglamentario. Es el procedimiento más detallado de los evaluados.

**Claro**

En su informe de sostenibilidad, Claro ofrece una tabla que detalla las normas y la autoridad competente referida a cada tipo de requerimiento de información. La entrega de datos, según la empresa, se realiza por solicitud de juez de control de garantías, por la Procuraduría General, la DIAN o cuando hay cobro coactivo de entidades públicas.

Además, Claro explica que antes de entregar la información requerida, evalúa que la entidad esté autorizada para hacer la solicitud. Así pues, decide si está obligada a entregar información y responde haciéndolo, solicitando en algunos casos más requisitos o rechazando la solicitud. El procedimiento de análisis de las solicitudes podría ser más específico.

---

*6. Ley 1581 de 2012 art. 10 y 13*
*7. Corte Constitucional. Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.*

**Tigo**

Informa que tiene un procedimiento interno para proteger los datos personales y en su informe de transparencia de 2017 ofrece una infografía sobre ese procedimiento que se consideró como vigente, pero no hay más datos sobre la forma como esto funciona. No menciona si notifica a las personas de estos requerimientos.

**Movistar** y **Claro** informan que tiene procedimientos y presentan detalles donde se sugieren medidas garantistas para las personas usuarias. Ahora bien, vale la pena mencionar que la forma como esta información se relaciona con el informe de transparencia difiere para las tres empresas. **Tigo** solo tiene la infografía pero está atada al informe de transparencia con datos de 2017. **Movistar** no da detalles pero da datos agregados de los requerimientos y **Claro** no ofrece ningún detalle. Ninguna de estas empresas notifica a sus clientes cuando se producen estos requerimientos.

**ETB**

No aparecen datos de un procedimiento interno para proteger los datos personales derivados de requerimientos de entidades públicas pero es la única empresa que si entrega detalles desagregados sobre esos requerimientos en su informe de transparencia, aunque esto no representa un punto en la evaluación acá sí queremos resaltarlo porque muestra la conexión que las empresas pueden hacer. ETB tampoco menciona si notifica a las personas de estos requerimientos.

**DirecTV**

DirecTV refiere que comparte datos personales con las autoridades cuando hay un requerimiento legal, pero no es claro respecto a los casos y normas que justifican esta entrega . Sin embargo, es el único que explica que "podría" notificar previamente a las personas cuando se produce un requerimiento legal, indica que lo hace con el propósito de darle la posibilidad a su cliente de defenderse, de averiguar sobre esa solicitud ante las autoridades competentes. Aunque esto es positivo, como la empresa indica que notificar a las personas es una posibilidad no se puede hablar de un compromiso, es sólo eso, una posibilidad.

## Recomendaciones

- Las empresas que dan acceso a internet custodian información de las personas a las que prestan servicios, por tanto deben explicar los procedimientos que usan para hacer efectivas las obligaciones legales. Esto incluye hacer explícitas las normas y los motivos que los obligan a realizar el procedimiento de entrega de datos, a entidades del sector público y quiénes son las autoridades legitimadas para pedirlos.

- Movistar y Claro, que cumplen con este criterio, pueden dar más información y pueden articular estas buenas prácticas con datos en el informe de transparencia sobre tipo de requerimiento, autoridad o la respuesta que dieron.

- Tigo puede mejorar la información vinculada con el procedimiento de requerimientos de información que hacen las autoridades para ampliar la información y

asegurarse que sea claro para quienes lo consultan que está vigente.

- Directv, ETB y EMCALI no tienen suficiente información para comunicar sobre los procedimientos de entrega de datos al sector público.

- En general las empresas pueden trabajar para dar más información sobre las bases legales y las razones por las que las empresas están obligadas a cumplir con solicitudes de datos personales por parte del sector público, el procedimiento que realizan y cómo defienden los derechos de las personas cuando suceden esas solicitudes.

- A excepción de Directv, ninguna empresa habla de notificar las solicitudes de datos a sus clientes. Como Karisma no evalúa prácticas sino que revisa lo que las empresas dicen que hacen esta "posibilidad" supone un reto para la evaluación. En 2019 volvimos a calificarla positivamente pero a futuro seguramente habrá que analizarlo. Creemos que esta empresa puede demostrar su compromiso más allá de la "posibilidad" dando más información.e indicando expresamente cuándo hace esta notificación (el tipo de casos por ejemplo), o a través del informe de transparencia demostrar que sí hace estas notificaciones. Es decir, se necesita que DirecTV indique como mínimo cuántas veces hizo uso de esta posibilidad en un período determinado, de lo contrario la política no es realmente un compromiso.

Notificar a los usuarios cuando una autoridad lo solicita puede ser difícil para los operadores colombianos porque hay un manto de silencio frente a los requerimientos de la autoridad pública. Este silencio afecta el derecho a la defensa de las personas y va en contravía de lo que sucede en otros países.

Notificar a las personas cuando una autoridad pública solicita sus datos es una práctica mundial.

En Estados Unidos las solicitudes de información son públicas a menos que la autoridad indique lo contrario. Esto seguramente explica la política de DIrecTV que repite lo que hace su matriz en ese país.

En un contexto más cercano al colombiano, en el informe ¿Quién defiende tus datos? de Chile, que realiza Derechos Digitales, se encontró que Claro Chile tiene una "política de requerimientos de información" según la cual, notifica a los usuarios cuando las autoridades piden información personal en procesos civiles, laborales y de familia. De esta forma ha limitado la reserva sólo a los procesos penales.

En Colombia no hay ninguna norma que ordene a las empresas no hacer esta notificación, por tanto este es un aspecto en el que todas las empresas pueden mejorar.

## ¿Cómo informan sobre sus políticas de protección de datos?

La recolección y análisis de datos personales se ha convertido en una fuente de ingreso a la que recurren las empresas. Este modelo de negocios trae consigo la responsabilidad de que ese uso quede expreso, por ejemplo en la política de protección de datos de cada operador.

### ¿Qué dice la ley?

Los datos personales sólo se pueden usar cuando la persona titular de los mismos ha sido informada sobre el empleo que le darán y ha dado su consentimiento[8]. La ley de protección de datos obliga a quien haga su tratamiento a tener una política de protección de los mismos, además debe solicitar autorización para ese tratamiento[9].

### ¿Qué informan los operadores?

En 2015, la primera vez que Karisma hizo esta evaluación, era normal que los documentos que publicaban las empresas fueran copias de la ley en formatos en los que no era posible siquiera buscar palabras. Durante estos cinco años, los operadores han mejorado la forma en que hacen esta publicación y han respondido bien a nuevos requerimientos que se hacen para la evaluación de ¿Dónde Están mis Datos?.

**Claro**

Tiene una política de protección de datos en la que se recoge la Ley de protección de datos pero no especifican cuáles y qué uso le dan a los que recogen.

**Movistar**

Cuenta con una política de privacidad en la que explica que recoge datos de tipo "demográfico, económico, biométricos, de servicios, comercial y de localización" y que los usará para los asuntos propios del contrato pero también para calcular el riesgo económico o crediticio, publicar directorios telefónicos, control y prevención del fraude. Sin embargo, no es claro qué significa "para beneficio propio o de terceros" con los que haya acuerdos con fines comerciales en Colombia o en el exterior.

**Tigo**

Posee una política de protección de datos personales en la que explica que recoge datos de registro, tales como nombre, número de teléfono, información de pago e información sobre el uso que dan las personas a su portal web, "información del uso de aplicaciones móviles según

---

*8. Ley 1581 de 2012. Ley de protección de datos. Artículos 4 y 8 sobre consentimiento y el derecho a ser informado sobre qué uso dan a los datos personales.*
*9. Ley 1581 de 2012. Ley de protección de datos. Artículos 12 y 17 sobre el deber de informar a las personas qué tratamiento dan a sus datos, para qué se recogen sus datos y qué derechos tiene en relación con este tratamiento de datos.*

los sitios web visitados y las aplicaciones descargadas de la red Tigo". Así mismo informa cómo obtiene esos datos, específicamente, la recolección directa y a través de *cookies* en su portal web. En el Aviso de privacidad la empresa manifiesta que hará el tratamiento de datos personales también para la protección de los derechos, la propiedad o la seguridad de Tigo, sus clientes, empleados o público en general. Sobre terceros, informa que entregará datos de acuerdo a la autorización y mediante orden escrita de autoridad judicial competente.

**DirecTV**

DirecTV tiene una política de protección de datos en la que clasifica qué datos recoge y cómo. Informa a sus clientes que acumula además de la información personal, información anónima y personal sobre el equipo recibidor o información sobre el uso del sitio web a través de *cookies*.

Explica cómo guardan la información y para qué la usan. Por ejemplo, exponen que usan los datos para "entender mejor lo que nuestros clientes quieren de modo que podamos continuar proveyendo un servicio de entretenimiento atractivo al mejor precio", es decir, hacen análisis de mercado y perfiles de consumo de las personas usuarias.

Finalmente, explican que comparten información, además de sus proveedores y para fines del servicio, con terceros para coordinar el cobro de servicios, con compañías afiliadas, con terceros dedicados al mercadeo. Con estos últimos, por ejemplo, anuncian que pueden compartir "información de programación vista anónima agregada", es decir, estadísticas sobre los programas de televisión vistos, no información individualizada sobre lo que cada cliente ve. Este tipo de detalles que da DirecTV muestra que es posible ser más precisos con los datos que recogen.

### Recomendaciones

- Las empresas que dan acceso a internet pueden ser más específicas en cómo informan sobre el tratamiento de datos de los usuarios; aunque refieren que los utilizarán de acuerdo con la autorización, no es claro en concreto qué usos están reglamentados. La explicación que hay en los documentos públicos así lo dejan ver.

- Ser más claros en qué signifca que harán tratamiento de datos para beneficio propio o de terceros. Se puede explicar mejor en qué consisten estos convenios con terceros.

## Otros criterios evaluados

La evaluación de ¿Dónde están mis datos? incluye otros temas:

**1. Los compromisos políticos de los operadores y el enfoque de género:** En este punto encontramos que algunas cosas no han cambiado respecto del 2018. Sin embargo, se puede resaltar que para 2019 hay compromisos más claros por la inclusión, el apoyo a las mujeres de sus equipos de trabajo en el desarrollo de sus carreras, y políticas para la prevención del acoso.

**2. Política de accesibilidad:** Sobre el compromiso para facilitar que poblaciones con necesidades especiales accedan a la información que entregan en línea se destacan nuevamente EMCALI y Mo-

vistar. En sus páginas web se encuentran opciones que permiten que personas con discapacidad accedan de manera sencilla a los contenidos que ofrecen estos dos operadores.

**3. Bloqueos de sitios web:** Su posición como intermediarios les da a los operadores una instancia privilegiada para influir en el acceso de las personas que usan sus servicios a contenidos y servicios de internet. Durante los años que llevamos haciendo esta evaluación hemos visto que anuncian las normas que aplican y nos informan sobre los procedimientos de bloqueo que siguen. Aunque hay otras causales de bloqueo en la ley colombiana, proveen más información en el tema de contenido de explotación sexual de menores que sobre cualquier otro.

La posición de intermediarios que tienen estas empresas está vinculada con la garantía de la neutralidad de la red. Ser transparentes y dar información sobre la forma como gestionan bloqueos por motivos de tráfico y por órdenes legales y judiciales es también un beneficio importante para estas empresas que pueden demostrar el buen manejo que hacen de su posición. Por eso Karisma cree que en este aspecto de la evaluación existe mucho espacio para mejorar. Uno de estos elementos es el aviso que las empresas ponen para informar a las personas que un sitio está bloqueado. En la evaluación de 2019 identificamos que este no siempre aparece y no siempre se explica la razón del bloqueo. Como en otros aspectos de este criterio también acá ofrecen más información cuando se trata de bloqueos por contenido de explotación sexual de menores.

Con posterioridad al Paro Nacional del 21 de noviembre de 2019, pero cuando todavía sentíamos su influencia, Karisma identificó un bloqueo al sitio web de RCN Radio. Como resultado, no se podía ingresar al contenido de esa página.

Al hacer algunos ejercicios de evaluación se estableció que el bloqueo se daba para las personas usuarias de Claro. El bloqueo desapareció durante la madrugada siguiente. Al informar este hecho a la empresa, Claro reportó que cuando ejecutó esa noche los bloqueos de sitios ilegales reportados por el Ministerio TIC, efectivamente sucedió el bloqueo a RCN Radio. La empresa explicó que el medio usaba el mismo servidor en Amazon de un sitio reportado como de apuestas ilegales por el Ministerio TIC. Claro explicó que ellos mismos identificaron el problema, e hicieron un ajuste técnico para evitar el bloqueo ilegítimo. El sitio regresó al aire durante la madrugada.

Tener ejercicios de transparencia permanentes puede ayudar a las empresas a evitar problemas reputacionales en temas que cada vez son más sensibles para las personas.

**4. Seguridad digital:** Es el tercer año en que se hace esta evaluación y es muy positivo constatar que hoy todos los operadores implementan https en sus portales web. Ahora bien, en relación con las vulnerabilidades y los incidentes de seguridad, es necesario que tengan compromisos más claros sobre cómo actúan en diferentes casos de este tipo y, sobre todo, expresar un compromiso abierto y claro de parte de los operadores de informar los incidentes de seguridad, no sólo a la Delegatura de Protección de Datos como es su deber legal, sino a sus clientes y al colCERT. En este campo Movistar es la que más información y detalles ofrece.



# Las gráficas ¿Dónde están mis datos?

Los datos de la evaluación de cada empresa se reflejan en las siguientes gráficas:

| Claro | SUMA POR CRITERIO | PROMEDIO POR EJE 2018 | PROMEDIO POR EJE 2019 |
|---|---|---|---|
| **1. COMPROMISOS POLÍTICOS** | | | |
| 1.1 Política de género | | | |
| 1.2. Política de accesibilidad | | | |
| 1.3. Informes de transparencia | | | |
| **2. INTIMIDAD** | | | |
| 2.1. Políticas de protección de datos | | | |
| 2.2. Informa la obligación legal de retención de datos | | | |
| 2.3. Informa las razones para responder a solicitudes de información del sector público | | | |
| 2.4. Procedimiento de entrega de datos al sector público | | | |
| 2.5. Notifica a las personas sobre la entrega de datos a entidades públicas | | | |
| 2.6 Criterios para el tratamiento de datos en relación con aliados comerciales | | | |
| **3. LIBERTAD DE EXPRESIÓN** | | | |
| 3.1. Informa sobre la obligación legal de bloqueo | | | |
| 3.2 Procedimientos de bloqueo (incluye obligación contractual) | | | |
| 3.3. Guía sobre comportamientos no permitidos | | | |
| **4. SEGURIDAD DIGITAL** | | | |
| 4.1. Informa de fuga de datos personales y acciones de mitigación | | | |
| 4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web | | | |

| Claro | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **1 COMPROMISOS POLÍTICOS** | | | | | | | **2** |
| **1.1 Política de género** | | | | | | **3** | |
| 1.1.1. Selección y contratación de personal (diversidad sexual y de género) | 1 | 1 | 1 | 1 | | **4** | |
| 1.1.2 Desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 1.1.3 Equilibrio familiar-laboral (e igualdad en beneficios) | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 1.1.4 Prevención del acoso sexual | 1 | 1 | 1 | 1 | | **4** | |
| 1.1.5 Promoción de imágenes públicas no sexistas | 0 | 0 | 0 | 0 | | **0** | |
| **1.2. Política de accesibilidad** | | | | | | **0** | |
| 1.2.1 La empresa pública en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos y de información de sus servicios para personas con discapacidad. | 0 | 0 | 0 | 0 | | **0** | |
| **1.3. Informes de transparencia** | | | | | | **4** | |
| 1.3.1. Solicitudes de datos del suscriptor (Decreto 1704 y Ley Inteligencia) donde se indica datos como: número de solicitudes, mes/año de solicitud, autoridad que solicita y número de solicitudes atendidas y no atendidas. | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 1.3.2. Bloqueos de URL o sitios web donde indica datos como: Solicitante (autoridad o titular de derechos), Motivo (pornografía, juegos, orden judicial, orden administrativa), Mes/Año de solicitud, Número de solicitudes atendidas y no atendidas y temporalidad del bloqueo: temporal o definitivo. | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 1.3.3. Interceptaciones de líneas telefónicas donde indica datos como: Tipo de servicio (fijo/móvil), Autoridad que solicita la interceptación, Duración de la interceptación, Número de solicitudes atendidas y no atendidas. | 1 | 1 | 0,5 | 1 | | **3,5** | |

| Claro | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **2. INTIMIDAD** | | | | | | | **2** |
| **2.1. Políticas de protección de datos** | | | | | | **3** | |
| 2.1.1 Publica en el sitio web para Colombia su política de protección de datos, y esa política es específica en indicar | 1 | 1 | 1 | 1 | | **4** | |
| 2.1.2 Qué datos recoge | 0 | 0 | 0 | 0 | | **0** | |
| 2.1.3 Cuáles son los usos que hace de los datos | 1 | 0,5 | 0,5 | 1 | | **3** | |
| 2.1.4 Qué terceros acceden a los datos que recoge | 1 | 0,5 | 0,5 | 1 | | **3** | |
| **2.2. Informa la obligación legal de retención de datos** | | | | | | **3** | |
| 2.2.1 que está obligada por ley a retener datos | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 2.2.2. el tipo de datos que retiene | 0 | 0 | 0 | 0 | | **0** | |
| 2.2.3 el tiempo por el que los retiene | 1 | 1 | 0,5 | 1 | | **3,5** | |
| **2.3. Informa las razones para responder a solicitudes de información del sector público** | | | | | | **4** | |
| La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada acordado cumplir con solicitudes de datos personales por parte del sector público. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa. | 1 | 1 | 0,5 | 1 | | **3,5** | |
| **2.4. Procedimiento de entrega de datos al sector público** | | | | | | **4** | |
| 2.4.1 Ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 2.4.2 Tiene mecanismos que garanticen los derechos de los usuarios | 1 | 1 | 0,5 | 1 | | **3,5** | |
| **2.5. Notifica a las personas sobre la entrega de datos a entidades públicas** | | | | | | **0** | |
| La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud por parte de un tercero | 0 | 0 | 0 | 0 | | **0** | |
| **2.6 Criterios para el tratamiento de datos en relación con aliados comerciales** | | | | | | **0** | |
| La empresa especifica los criterios para decidir con qué aliados comerciales y en qué condiciones comparte datos personales de sus usuarios | 0 | 0 | 0 | 0 | | **0** | |

| Claro | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **3. LIBERTAD DE EXPRESIÓN** | | | | | | | **3** |
| **3.1. Informa sobre la obligación legal de bloqueo** | | | | | | **4** | |
| 3.1.1 Informa si bloquea contenidos por explotación de personas menores de edad, juegos de suerte y azar y órdenes judiciales. | 1 | 1 | 0,5 | 1 | | 3,5 | |
| 3.1.2 Informa el soporte legal | 1 | 1 | 0,5 | 1 | | 3,5 | |
| **3.2 Procedimientos de bloqueo (incluye obligación contractual)** | | | | | | **2** | |
| 3.2.1. Informa el procedimiento que sigue para el bloqueo según los criterios que emplea para filtrar, retirar o bloquear contenidos (legales y contractuales), | 1 | 1 | 0,5 | 1 | | 3,5 | |
| 3.2.2 Cuando bloquea por motivos contractuales tiene un procedimiento de queja para los usuarios | 0 | 0 | 0 | 0 | | 0 | |
| 3.2.3 Anuncia a usuarios el motivo del bloqueo | 1 | 0,5 | 1 | 1 | | 3,5 | |
| **3.3. Guía sobre comportamientos no permitidos** | | | | | | **4** | |
| La empresa pública en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones | 1 | 1 | 0,5 | 1 | | 3,5 | |
| **4. SEGURIDAD DIGITAL** | | | | | | | **2** |
| **4.1. Informa de fuga de datos personales y acciones de mitigación** | | | | | | **0** | |
| 4.1.1 Notificación sin demora indebida a las autoridades pertinentes | 0 | 0 | 0 | 0 | | 0 | |
| 4.1.2 Notificación a las personas afectadas | 0 | 0 | 0 | 0 | | 0 | |
| 4.1.3 El tipo de medidas que la empresa puede tomar para mitigar los daños | 0 | 0 | 0 | 0 | | 0 | |
| **4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web** | | | | | | **4** | |
| | 1 | 1 | 1 | 1 | | 4 | |

| EMCALI | SUMA POR CRITERIO | PROMEDIO POR EJE | |
|---|---|---|---|
| | | 2018 | 2019 |
| **1. COMPROMISOS POLÍTICOS** | | | |
| 1.1 Política de género | | | |
| 1.2. Política de accesibilidad | | | |
| 1.3. Informes de transparencia | | | |
| **2. INTIMIDAD** | | | |
| 2.1. Políticas de protección de datos | | | |
| 2.2. Informa la obligación legal de retención de datos | | | |
| 2.3. Informa las razones para responder a solicitudes de información del sector público | | | |
| 2.4. Procedimiento de entrega de datos al sector público | | | |
| 2.5. Notifica a las personas sobre la entrega de datos a entidades públicas | | | |
| 2.6 Criterios para el tratamiento de datos en relación con aliados comerciales | | | |
| **3. LIBERTAD DE EXPRESIÓN** | | | |
| 3.1. Informa sobre la obligación legal de bloqueo | | | |
| 3.2 Procedimientos de bloqueo (incluye obligación contractual) | | | |
| 3.3. Guía sobre comportamientos no permitidos | | | |
| **4. SEGURIDAD DIGITAL** | | | |
| 4.1. Informa de fuga de datos personales y acciones de mitigación | | | |
| 4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web | | | |

| EMCALI | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **1 COMPROMISOS POLÍTICOS** | | | | | | | **1** |
| **1.1 Política de género** | | | | | | **0** | |
| 1.1.1. Selección y contratación de personal (diversidad sexual y de género) | 0 | 0 | 0 | 0 | | 0 | |
| 1.1.2 Desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos | 0 | 0 | 0 | 0 | | 0 | |
| 1.1.3 Equilibrio familiar-laboral (e igualdad en beneficios) | 0 | 0 | 0 | 0 | | 0 | |
| 1.1.4 Prevención del acoso sexual | 0 | 0 | 0 | 0 | | 0 | |
| 1.1.5 Promoción de imágenes públicas no sexistas | 0 | 0 | 0 | 0 | | 0 | |
| **1.2. Política de accesibilidad** | | | | | | **4** | |
| 1.2.1 La empresa pública en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos y de información de sus servicios para personas con discapacidad. | 1 | 1 | 1 | 1 | | 4 | |
| **1.3. Informes de transparencia** | | | | | | **0** | |
| 1.3.1. Solicitudes de datos del suscriptor (Decreto 1704 y Ley Inteligencia) donde se indica datos como: número de solicitudes, mes/año de solicitud, autoridad que solicita y número de solicitudes atendidas y no atendidas. | 0 | 0 | 0 | 0 | | 0 | |
| 1.3.2. Bloqueos de URL o sitios web donde indica datos como: Solicitante (autoridad o titular de derechos), Motivo (pornografía, juegos, orden judicial, orden administrativa), Mes/Año de solicitud, Número de solicitudes atendidas y no atendidas y temporalidad del bloqueo: temporal o definitivo. | 0 | 0 | 0 | 0 | | 0 | |
| 1.3.3. Interceptaciones de líneas telefónicas donde indica datos como: Tipo de servicio (fijo/móvil), Autoridad que solicita la interceptación, Duración de la interceptación, Número de solicitudes atendidas y no atendidas. | 0 | 0 | 0 | 0 | | 0 | |

| EMCALI | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **2. INTIMIDAD** | | | | | | | **0** |
| **2.1. Políticas de protección de datos** | | | | | | **1** | |
| 2.1.1 Publica en el sitio web para Colombia su política de protección de datos, y esa política es específica en indicar | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.2 Qué datos recoge | 0 | 0 | 0 | 0 | | 0 | |
| 2.1.3 Cuáles son los usos que hace de los datos | 0 | 0 | 0 | 0 | | 0 | |
| 2.1.4 Qué terceros acceden a los datos que recoge | 0 | 0 | 0 | 0 | | 0 | |
| **2.2. Informa la obligación legal de retención de datos** | | | | | | **0** | |
| 2.2.1 que está obligada por ley a retener datos | 0 | 0 | 0 | 0 | | 0 | |
| 2.2.2. el tipo de datos que retiene | 0 | 0 | 0 | 0 | | 0 | |
| 2.2.3 el tiempo por el que los retiene | 0 | 0 | 0 | 0 | | 0 | |
| **2.3. Informa las razones para responder a solicitudes de información del sector público** | | | | | | **0** | |
| La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada acordado cumplir con solicitudes de datos personales por parte del sector público. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa. | 0 | 0 | 0 | 0 | | 0 | |
| **2.4. Procedimiento de entrega de datos al sector público** | | | | | | **0** | |
| 2.4.1 Ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes | 0 | 0 | 0 | 0 | | 0 | |
| 2.4.2 Tiene mecanismos que garanticen los dere- | 0 | 0 | 0 | 0 | | 0 | |
| **2.5. Notifica a las personas sobre la entrega de datos a entidades públicas** | | | | | | **0** | |
| La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud | 0 | 0 | 0 | 0 | | 0 | |
| **2.6 Criterios para el tratamiento de datos en relación con aliados comerciales** | | | | | | **0** | |
| La empresa especifica los criterios para decidir con qué aliados comerciales y en qué condiciones comparte datos personales de sus usuarios | 0 | 0 | 0 | 0 | | 0 | |

| EMCALI | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **3. LIBERTAD DE EXPRESIÓN** | | | | | | | **0** |
| **3.1. Informa sobre la obligación legal de bloqueo** | | | | | | **1** | |
| 3.1.1 Informa si bloquea contenidos por explotación de personas menores de edad, juegos de suerte y azar y órdenes judiciales. | 1 | 0,33 | 0,33 | 1 | | **2,33** | |
| 3.1.2 Informa el soporte legal | 0 | 0 | 0 | 0 | | **0** | |
| **3.2 Procedimientos de bloqueo (incluye obligación contractual)** | | | | | | **0** | |
| 3.2.1. Informa el procedimiento que sigue para el bloqueo según los criterios que emplea para filtrar, retirar o bloquear contenidos (legales y contractuales), | 0 | 0 | 0 | 0 | | **0** | |
| 3.2.2 Cuando bloquea por motivos contractuales tiene un procedimiento de queja para los usuarios | 0 | 0 | 0 | 0 | | **0** | |
| 3.2.3 Anuncia a usuarios el motivo del bloqueo | 0 | 0 | 0 | 0 | | **0** | |
| **3.3. Guía sobre comportamientos no permitidos** | | | | | | **0** | |
| La empresa pública en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones | 0 | 0 | 0 | 0 | | **0** | |
| **4. SEGURIDAD DIGITAL** | | | | | | | **2** |
| **4.1. Informa de fuga de datos personales y acciones de mitigación** | | | | | | **0** | |
| 4.1.1 Notificación sin demora indebida a las autoridades pertinentes | 0 | 0 | 0 | 0 | | **0** | |
| 4.1.2 Notificación a las personas afectadas | 0 | 0 | 0 | 0 | | **0** | |
| 4.1.3 El tipo de medidas que la empresa puede tomar para mitigar los daños | 0 | 0 | 0 | 0 | | **0** | |
| **4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web** | | | | | | **4** | |
| | 1 | 1 | 1 | 1 | | **4** | |

| movistar | SUMA POR CRITERIO | PROMEDIO POR EJE | |
| --- | --- | --- | --- |
| | | 2018 | 2019 |
| **1. COMPROMISOS POLÍTICOS** | | | |
| 1.1 Política de género | | | |
| 1.2. Política de accesibilidad | | | |
| 1.3. Informes de transparencia | | | |
| **2. INTIMIDAD** | | | |
| 2.1. Políticas de protección de datos | | | |
| 2.2. Informa la obligación legal de retención de datos | | | |
| 2.3. Informa las razones para responder a solicitudes de información del sector público | | | |
| 2.4. Procedimiento de entrega de datos al sector público | | | |
| 2.5. Notifica a las personas sobre la entrega de datos a entidades públicas | | | |
| 2.6 Criterios para el tratamiento de datos en relación con aliados comerciales | | | |
| **3. LIBERTAD DE EXPRESIÓN** | | | |
| 3.1. Informa sobre la obligación legal de bloqueo | | | |
| 3.2 Procedimientos de bloqueo (incluye obligación contractual) | | | |
| 3.3. Guía sobre comportamientos no permitidos | | | |
| **4. SEGURIDAD DIGITAL** | | | |
| 4.1. Informa de fuga de datos personales y acciones de mitigación | | | |
| 4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web | | | |

movistar

| | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **1 COMPROMISOS POLÍTICOS** | | | | | | | **4** |
| **1.1 Política de género** | | | | | | **4** | |
| 1.1.1. Selección y contratación de personal (diversidad sexual y de género) | 1 | 1 | 0,5 | 1 | ⚡ | **3,5** | |
| 1.1.2 Desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 1.1.3 Equilibrio familiar-laboral (e igualdad en beneficios) | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 1.1.4 Prevención del acoso sexual | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 1.1.5 Promoción de imágenes públicas no sexistas | 1 | 1 | 0,5 | 1 | | **3,5** | |
| **1.2. Política de accesibilidad** | | | | | | **4** | |
| 1.2.1 La empresa pública en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos y de información de sus servicios para personas con discapacidad. | 1 | 1 | 0,5 | 1 | | **3,5** | |
| **1.3. Informes de transparencia** | | | | | | **4** | |
| 1.3.1. Solicitudes de datos del suscriptor (Decreto 1704 y Ley Inteligencia) donde se indica datos como: número de solicitudes, mes/año de solicitud, autoridad que solicita y número de solicitudes atendidas y no atendidas. | 1 | 1 | 1 | 1 | | **4** | |
| 1.3.2. Bloqueos de URL o sitios web donde indica datos como: Solicitante (autoridad o titular de derechos), Motivo (pornografía, juegos, orden judicial, orden administrativa), Mes/Año de solicitud, Número de solicitudes atendidas y no atendidas y temporalidad del bloqueo: temporal o definitivo. | 1 | 1 | 1 | 1 | | **4** | |
| 1.3.3. Interceptaciones de líneas telefónicas donde indica datos como: Tipo de servicio (fijo/móvil), Autoridad que solicita la interceptación, Duración de la interceptación, Número de solicitudes atendidas y no atendidas. | 1 | 1 | 1 | 1 | | **4** | |

| movistar | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **2. INTIMIDAD** | | | | | | | **2** |
| **2.1. Políticas de protección de datos** | | | | | | **4** | |
| 2.1.1 Publica en el sitio web para Colombia su política de protección de datos, y esa política es específica en indicar | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.2 Qué datos recoge | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.3 Cuáles son los usos que hace de los datos | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.4 Qué terceros acceden a los datos que recoge | 1 | 1 | 1 | 1 | | 4 | |
| **2.2. Informa la obligación legal de retención de datos** | | | | | | **2** | |
| 2.2.1 que está obligada por ley a retener datos | 1 | 0 | 1 | 0 | | 2 | |
| 2.2.2. el tipo de datos que retiene | 1 | 1 | 1 | 1 | | 4 | |
| 2.2.3 el tiempo por el que los retiene | 1 | 0,5 | 1 | 0 | | 2,5 | |
| **2.3. Informa las razones para responder a solicitudes de información del sector público** | | | | | | **4** | |
| La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada acordado cumplir con solicitudes de datos personales por parte del sector público. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa. | 1 | 1 | 1 | 1 | | 4 | |
| **2.4. Procedimiento de entrega de datos al sector público** | | | | | | **0** | |
| 2.4.1 Ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes | 1 | 1 | 1 | 1 | | 4 | |
| 2.4.2 Tiene mecanismos que garanticen los derechos de los usuarios | 1 | 0,5 | 0,5 | 1 | | 3 | |
| **2.5. Notifica a las personas sobre la entrega de datos a entidades públicas** | | | | | | **0** | |
| La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud por parte de un tercero | 0 | 0 | 0 | 0 | | 0 | |
| **2.6 Criterios para el tratamiento de datos en relación con aliados comerciales** | | | | | | **0** | |
| La empresa especifica los criterios para decidir con qué aliados comerciales y en qué condiciones comparte datos personales de sus usuarios | 0 | 0 | 0 | 0 | | 0 | |

| movistar | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **3. LIBERTAD DE EXPRESIÓN** | | | | | | | **4** |
| **3.1. Informa sobre la obligación legal de bloqueo** | | | | | | **4** | |
| 3.1.1 Informa si bloquea contenidos por explotación de personas menores de edad, juegos de suerte y azar y órdenes judiciales. | 1 | 1 | 1 | 1 | | 4 | |
| 3.1.2 Informa el soporte legal | 1 | 1 | 1 | 1 | | 4 | |
| **3.2 Procedimientos de bloqueo (incluye obligación contractual)** | | | | | | **4** | |
| 3.2.1. Informa el procedimiento que sigue para el bloqueo según los criterios que emplea para filtrar, retirar o bloquear contenidos (legales y contractuales), | 1 | 1 | 1 | 1 | | 4 | |
| 3.2.2 Cuando bloquea por motivos contractuales tiene un procedimiento de queja para los usuarios | 1 | 1 | 1 | 1 | | 4 | |
| 3.2.3 Anuncia a usuarios el motivo del bloqueo | 1 | 0,5 | 1 | 1 | | 3,5 | |
| **3.3. Guía sobre comportamientos no permitidos** | | | | | | **4** | |
| La empresa pública en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones | 1 | 1 | 1 | 1 | | 4 | |
| **4. SEGURIDAD DIGITAL** | | | | | | | **4** |
| **4.1. Informa de fuga de datos personales y acciones de mitigación** | | | | | | **4** | |
| 4.1.1 Notificación sin demora indebida a las autoridades pertinentes | 1 | 0,5 | 1 | 1 | | 3,5 | |
| 4.1.2 Notificación a las personas afectadas | 1 | 1 | 1 | 1 | | 4 | |
| 4.1.3 El tipo de medidas que la empresa puede tomar para mitigar los daños | 1 | 1 | 1 | 1 | | 4 | |
| **4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web** | | | | | | **4** | |
| | 1 | 1 | 1 | 1 | | 4 | |

| tigo | SUMA POR CRITERIO | PROMEDIO POR EJE | |
|---|---|---|---|
| | | 2018 | 2019 |
| **1. COMPROMISOS POLÍTICOS** | | | |
| 1.1 Política de género | | | |
| 1.2. Política de accesibilidad | | | |
| 1.3. Informes de transparencia | | | |
| **2. INTIMIDAD** | | | |
| 2.1. Políticas de protección de datos | | | |
| 2.2. Informa la obligación legal de retención de datos | | | |
| 2.3. Informa las razones para responder a solicitudes de información del sector público | | | |
| 2.4. Procedimiento de entrega de datos al sector público | | | |
| 2.5. Notifica a las personas sobre la entrega de datos a entidades públicas | | | |
| 2.6 Criterios para el tratamiento de datos en relación con aliados comerciales | | | |
| **3. LIBERTAD DE EXPRESIÓN** | | | |
| 3.1. Informa sobre la obligación legal de bloqueo | | | |
| 3.2 Procedimientos de bloqueo (incluye obligación contractual) | | | |
| 3.3. Guía sobre comportamientos no permitidos | | | |
| **4. SEGURIDAD DIGITAL** | | | |
| 4.1. Informa de fuga de datos personales y acciones de mitigación | | | |
| 4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web | | | |

| tigo | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **1 COMPROMISOS POLÍTICOS** | | | | | | | **1** |
| **1.1 Política de género** | | | | | | **3** | |
| 1.1.1. Selección y contratación de personal (diversidad sexual y de género) | 1 | 1 | 0,5 | 1 | | 3,5 | |
| 1.1.2 Desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos | 1 | 1 | 0 | 1 | | 3 | |
| 1.1.3 Equilibrio familiar-laboral (e igualdad en beneficios) | 1 | 1 | 0 | 1 | | 3 | |
| 1.1.4 Prevención del acoso sexual | 1 | 1 | 0 | 1 | | 3 | |
| 1.1.5 Promoción de imágenes públicas no sexistas | 0 | 0 | 0 | 0 | | 0 | |
| **1.2. Política de accesibilidad** | | | | | | **0** | |
| 1.2.1 La empresa pública en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos y de información de sus servicios para personas con discapacidad. | 0 | 0 | 0 | 0 | | 0 | |
| **1.3. Informes de transparencia** | | | | | | **0** | |
| 1.3.1. Solicitudes de datos del suscriptor (Decreto 1704 y Ley Inteligencia) donde se indica datos como: número de solicitudes, mes/año de solicitud, autoridad que solicita y número de solicitudes atendidas y no atendidas. | 0 | 0 | 0 | 0 | | 0 | |
| 1.3.2. Bloqueos de URL o sitios web donde indica datos como: Solicitante (autoridad o titular de derechos), Motivo (pornografía, juegos, orden judicial, orden administrativa), Mes/Año de solicitud, Número de solicitudes atendidas y no atendidas y temporalidad del bloqueo: temporal o definitivo. | 0 | 0 | 0 | 0 | | 0 | |
| 1.3.3. Interceptaciones de líneas telefónicas donde indica datos como: Tipo de servicio (fijo/móvil), Autoridad que solicita la interceptación, Duración de la interceptación, Número de solicitudes atendidas y no atendidas. | 0 | 0 | 0 | 0 | | 0 | |

| tigo | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **2. INTIMIDAD** | | | | | | | **3** |
| **2.1. Políticas de protección de datos** | | | | | | **4** | |
| 2.1.1 Publica en el sitio web para Colombia su política de protección de datos, y esa política es específica en indicar | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.2 Qué datos recoge | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.3 Cuáles son los usos que hace de los datos | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.4 Qué terceros acceden a los datos que recoge | 1 | 1 | 1 | 1 | | 4 | |
| **2.2. Informa la obligación legal de retención de datos** | | | | | | **3** | |
| 2.2.1 que está obligada por ley a retener datos | 1 | 1 | 1 | 1 | | 4 | |
| 2.2.2. el tipo de datos que retiene | 0 | 0 | 0 | 0 | | 0 | |
| 2.2.3 el tiempo por el que los retiene | 1 | 0,5 | 1 | 1 | | 3,5 | |
| **2.3. Informa las razones para responder a solicitudes de información del sector público** | | | | | | **4** | |
| La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada acordado cumplir con solicitudes de datos personales por parte del sector público. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa. | 1 | 1 | 1 | 1 | | 4 | |
| **2.4. Procedimiento de entrega de datos al sector público** | | | | | | **1** | |
| 2.4.1 Ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes | 1 | 0 | 0,5 | 0 | | 1,5 | |
| 2.4.2 Tiene mecanismos que garanticen los dere- | 0 | 0 | 0 | 0 | | 0 | |
| **2.5. Notifica a las personas sobre la entrega de datos a entidades públicas** | | | | | | **0** | |
| La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud por parte de un tercero | 0 | 0 | 0 | 0 | | 0 | |
| **2.6 Criterios para el tratamiento de datos en relación con aliados comerciales** | | | | | | **4** | |
| La empresa especifica los criterios para decidir con qué aliados comerciales y en qué condiciones comparte datos personales de sus usuarios | 1 | 1 | 1 | 1 | | 4 | |

| tigo | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **3. LIBERTAD DE EXPRESIÓN** | | | | | | | **4** |
| **3.1. Informa sobre la obligación legal de bloqueo** | | | | | | **4** | |
| 3.1.1 Informa si bloquea contenidos por explotación de personas menores de edad, juegos de suerte y azar y órdenes judiciales. | 1 | 1 | 1 | 1 | | 4 | |
| 3.1.2 Informa el soporte legal | 1 | 1 | 1 | 1 | | 4 | |
| **3.2 Procedimientos de bloqueo (incluye obligación contractual)** | | | | | | **4** | |
| 3.2.1. Informa el procedimiento que sigue para el bloqueo según los criterios que emplea para filtrar, retirar o bloquear contenidos (legales y contractuales), | 1 | 0,66 | 1 | 1 | | 3,66 | |
| 3.2.2 Cuando bloquea por motivos contractuales tiene un procedimiento de queja para los usuarios | 1 | 0,5 | 1 | 1 | | 3,5 | |
| 3.2.3 Anuncia a usuarios el motivo del bloqueo | 1 | 0,5 | 1 | 1 | | 3,5 | |
| **3.3. Guía sobre comportamientos no permitidos** | | | | | | **4** | |
| La empresa pública en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones | 1 | 1 | 1 | 1 | | 4 | |
| **4. SEGURIDAD DIGITAL** | | | | | | | **2** |
| **4.1. Informa de fuga de datos personales y acciones de mitigación** | | | | | | **0** | |
| 4.1.1 Notificación sin demora indebida a las autoridades pertinentes | 0 | 0 | 0 | 0 | | 0 | |
| 4.1.2 Notificación a las personas afectadas | 0 | 0 | 0 | 0 | | 0 | |
| 4.1.3 El tipo de medidas que la empresa puede tomar para mitigar los daños | 0 | 0 | 0 | 0 | | 0 | |
| **4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web** | | | | | | **4** | |
| | 1 | 1 | 1 | 1 | | 4 | |

| | SUMA POR CRITERIO | PROMEDIO POR EJE 2018 | PROMEDIO POR EJE 2019 |
|---|---|---|---|
| **1. COMPROMISOS POLÍTICOS** | | | |
| 1.1 Política de género | | | |
| 1.2. Política de accesibilidad | | | |
| 1.3. Informes de transparencia | | | |
| **2. INTIMIDAD** | | | |
| 2.1. Políticas de protección de datos | | | |
| 2.2. Informa la obligación legal de retención de datos | | | |
| 2.3. Informa las razones para responder a solicitudes de información del sector público | | | |
| 2.4. Procedimiento de entrega de datos al sector público | | | |
| 2.5. Notifica a las personas sobre la entrega de datos a entidades públicas | | | |
| 2.6 Criterios para el tratamiento de datos en relación con aliados comerciales | | | |
| **3. LIBERTAD DE EXPRESIÓN** | | | |
| 3.1. Informa sobre la obligación legal de bloqueo | | | |
| 3.2 Procedimientos de bloqueo (incluye obligación contractual) | | | |
| 3.3. Guía sobre comportamientos no permitidos | | | |
| **4. SEGURIDAD DIGITAL** | | | |
| 4.1. Informa de fuga de datos personales y acciones de mitigación | | | |
| 4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web | | | |

| ETB | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **1 COMPROMISOS POLÍTICOS** | | | | | | | **2** |
| **1.1 Política de género** | | | | | | **2** | |
| 1.1.1. Selección y contratación de personal (diversidad sexual y de género) | 1 | 1 | 0,5 | 0 | | **2,5** | |
| 1.1.2 Desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos | 1 | 1 | 0,5 | 0 | | **2,5** | |
| 1.1.3 Equilibrio familiar-laboral (e igualdad en beneficios) | 0 | 0 | 0 | 0 | | **0** | |
| 1.1.4 Prevención del acoso sexual | 1 | 1 | 0,5 | 0 | | **2,5** | |
| 1.1.5 Promoción de imágenes públicas no sexistas | 0 | 0 | 0 | 0 | | **0** | |
| **1.2. Política de accesibilidad** | | | | | | **0** | |
| 1.2.1 La empresa pública en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos y de información de sus servicios para personas con discapacidad. | 0 | 0 | 0 | 0 | | **0** | |
| **1.3. Informes de transparencia** | | | | | | **3** | |
| 1.3.1. Solicitudes de datos del suscriptor (Decreto 1704 y Ley Inteligencia) donde se indica datos como: número de solicitudes, mes/año de solicitud, autoridad que solicita y número de solicitudes atendidas y no atendidas. | 1 | 1 | 0,5 | 0 | | **2,5** | |
| 1.3.2. Bloqueos de URL o sitios web donde indica datos como: Solicitante (autoridad o titular de derechos), Motivo (pornografía, juegos, orden judicial, orden administrativa), Mes/Año de solicitud, Número de solicitudes atendidas y no atendidas y temporalidad del bloqueo: temporal o definitivo. | 1 | 1 | 0,5 | 0 | | **2,5** | |
| 1.3.3. Interceptaciones de líneas telefónicas donde indica datos como: Tipo de servicio (fijo/móvil), Autoridad que solicita la interceptación, Duración de la interceptación, Número de solicitudes atendidas y no atendidas. | 1 | 0,5 | 0,5 | 1 | | **2,5** | |

| etb | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **2. INTIMIDAD** | | | | | | | **0** |
| **2.1. Políticas de protección de datos** | | | | | | **1** | |
| 2.1.1 Publica en el sitio web para Colombia su política de protección de datos, y esa política es específica en indicar | 1 | 1 | 0,5 | 1 | | 3,5 | |
| 2.1.2 Qué datos recoge | 0 | 0 | 0 | 0 | | 0 | |
| 2.1.3 Cuáles son los usos que hace de los datos | 0 | 0 | 0 | 0 | | 0 | |
| 2.1.4 Qué terceros acceden a los datos que recoge | 0 | 0 | 0 | 0 | | 0 | |
| **2.2. Informa la obligación legal de retención de datos** | | | | | | **1** | |
| 2.2.1 que está obligada por ley a retener datos | 1 | 0,2 | 0,5 | 1 | | 2,27 | |
| 2.2.2. el tipo de datos que retiene | 0 | 0 | 0 | 0 | | 0 | |
| 2.2.3 el tiempo por el que los retiene | 0 | 0 | 0 | 0 | | 0 | |
| **2.3. Informa las razones para responder a solicitudes de información del sector público** | | | | | | **0** | |
| La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada acordado cumplir con solicitudes de datos personales por parte del sector público. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa. | 0 | 0 | 0 | 0 | | 0 | |
| **2.4. Procedimiento de entrega de datos al sector público** | | | | | | **0** | |
| 2.4.1 Ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes | 0 | 0 | 0 | 0 | | 0 | |
| 2.4.2 Tiene mecanismos que garanticen los derechos de los usuarios | 0 | 0 | 0 | 0 | | 0 | |
| **2.5. Notifica a las personas sobre la entrega de datos a entidades públicas** | | | | | | **0** | |
| La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud por parte de un tercero | 0 | 0 | 0 | 0 | | 0 | |
| **2.6 Criterios para el tratamiento de datos en relación con aliados comerciales** | | | | | | **0** | |
| La empresa especifica los criterios para decidir con qué aliados comerciales y en qué condiciones comparte datos personales de sus usuarios | 0 | 0 | 0 | 0 | | 0 | |

| ETB | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **3. LIBERTAD DE EXPRESIÓN** | | | | | | | **3** |
| **3.1. Informa sobre la obligación legal de bloqueo** | | | | | | **4** | |
| 3.1.1 Informa si bloquea contenidos por explotación de personas menores de edad, juegos de suerte y azar y órdenes judiciales. | 1 | 1 | 0,5 | 1 | | **3,5** | |
| 3.1.2 Informa el soporte legal | 1 | 1 | 0,5 | 1 | | **3,5** | |
| **3.2 Procedimientos de bloqueo (incluye obligación contractual)** | | | | | | **1** | |
| 3.2.1. Informa el procedimiento que sigue para el bloqueo según los criterios que emplea para filtrar, retirar o bloquear contenidos (legales y contractuales), | 0 | 0 | 0 | 0 | | **0** | |
| 3.2.2 Cuando bloquea por motivos contractuales tiene un procedimiento de queja para los usuarios | 0 | 0 | 0 | 0 | | **0** | |
| 3.2.3 Anuncia a usuarios el motivo del bloqueo | 1 | 0,5 | 1 | 1 | | **3,5** | |
| **3.3. Guía sobre comportamientos no permitidos** | | | | | | **4** | |
| La empresa pública en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones | 1 | 1 | 0,5 | 1 | | **3,5** | |
| **4. SEGURIDAD DIGITAL** | | | | | | | **2** |
| **4.1. Informa de fuga de datos personales y acciones de mitigación** | | | | | | **0** | |
| 4.1.1 Notificación sin demora indebida a las autoridades pertinentes | 0 | 0 | 0 | 0 | | **0** | |
| 4.1.2 Notificación a las personas afectadas | 0 | 0 | 0 | 0 | | **0** | |
| 4.1.3 El tipo de medidas que la empresa puede tomar para mitigar los daños | 0 | 0 | 0 | 0 | | **0** | |
| **4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web** | | | | | | **4** | |
| | 1 | 1 | 1 | 1 | | **4** | |

| DIRECTV | SUMA POR CRITERIO | PROMEDIO POR EJE | |
|---|---|---|---|
| | | 2018 | 2019 |
| **1. COMPROMISOS POLÍTICOS** | | | |
| 1.1 Política de género | | | |
| 1.2. Política de accesibilidad | | | |
| 1.3. Informes de transparencia | | | |
| **2. INTIMIDAD** | | | |
| 2.1. Políticas de protección de datos | | | |
| 2.2. Informa la obligación legal de retención de datos | | | |
| 2.3. Informa las razones para responder a solicitudes de información del sector público | | | |
| 2.4. Procedimiento de entrega de datos al sector público | | | |
| 2.5. Notifica a las personas sobre la entrega de datos a entidades públicas | | | |
| 2.6 Criterios para el tratamiento de datos en relación con aliados comerciales | | | |
| **3. LIBERTAD DE EXPRESIÓN** | | | |
| 3.1. Informa sobre la obligación legal de bloqueo | | | |
| 3.2 Procedimientos de bloqueo (incluye obligación contractual) | | | |
| 3.3. Guía sobre comportamientos no permitidos | | | |
| **4. SEGURIDAD DIGITAL** | | | |
| 4.1. Informa de fuga de datos personales y acciones de mitigación | | | |
| 4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web | | | |

| DIRECTV | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **1 COMPROMISOS POLÍTICOS** | | | | | | | **1** |
| **1.1 Política de género** | | | | | | **2** | |
| 1.1.1. Selección y contratación de personal (diversidad sexual y de género) | 1 | 1 | 1 | 1 | | 4 | |
| 1.1.2 Desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos | 0 | 0 | 0 | 0 | | 0 | |
| 1.1.3 Equilibrio familiar-laboral (e igualdad en beneficios) | 0 | 0 | 0 | 0 | | 0 | |
| 1.1.4 Prevención del acoso sexual | 1 | 1 | 1 | 1 | | 4 | |
| 1.1.5 Promoción de imágenes públicas no sexistas | 0 | 0 | 0 | 0 | | 0 | |
| **1.2. Política de accesibilidad** | | | | | | **0** | |
| 1.2.1 La empresa pública en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos y de información de sus servicios para personas con discapacidad. | 0 | 0 | 0 | 0 | | 0 | |
| **1.3. Informes de transparencia** | | | | | | **0** | |
| 1.3.1. Solicitudes de datos del suscriptor (Decreto 1704 y Ley Inteligencia) donde se indica datos como: número de solicitudes, mes/año de solicitud, autoridad que solicita y número de solicitudes atendidas y no atendidas. | 0 | 0 | 0 | 0 | | 0 | |
| 1.3.2. Bloqueos de URL o sitios web donde indica datos como: Solicitante (autoridad o titular de derechos), Motivo (pornografía, juegos, orden judicial, orden administrativa), Mes/Año de solicitud, Número de solicitudes atendidas y no atendidas y temporalidad del bloqueo: temporal o definitivo. | 0 | 0 | 0 | 0 | | 0 | |
| 1.3.3. Interceptaciones de líneas telefónicas donde indica datos como: Tipo de servicio (fijo/móvil), Autoridad que solicita la interceptación, Duración de la interceptación, Número de solicitudes atendidas y no atendidas. | 0 | 0 | 0 | 0 | | 0 | |

DIRECTV

| | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **2. INTIMIDAD** | | | | | | | **2** |
| **2.1. Políticas de protección de datos** | | | | | | **4** | |
| 2.1.1 Publica en el sitio web para Colombia su política de protección de datos, y esa política es específica en indicar | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.2 Qué datos recoge | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.3 Cuáles son los usos que hace de los datos | 1 | 1 | 1 | 1 | | 4 | |
| 2.1.4 Qué terceros acceden a los datos que recoge | 1 | 1 | 1 | 1 | | 4 | |
| **2.2. Informa la obligación legal de retención de datos** | | | | | | **1** | |
| 2.2.1 que está obligada por ley a retener datos | 0 | 0 | 0 | 0 | | 0 | |
| 2.2.2. el tipo de datos que retiene | 0 | 0 | 0 | 0 | | 0 | |
| 2.2.3 el tiempo por el que los retiene | 1 | 0,5 | 1 | 1 | | 3,5 | |
| **2.3. Informa las razones para responder a solicitudes de información del sector público** | | | | | | **0** | |
| La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada acordado cumplir con solicitudes de datos personales por parte del sector público. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa. | 0 | 0 | 0 | 0 | | 0 | |
| **2.4. Procedimiento de entrega de datos al sector público** | | | | | | **0** | |
| 2.4.1 Ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes | 0 | 0 | 0 | 0 | | 0 | |
| 2.4.2 Tiene mecanismos que garanticen los derechos de los usuarios | 0 | 0 | 0 | 0 | | 0 | |
| **2.5. Notifica a las personas sobre la entrega de datos a entidades públicas** | | | | | | **4** | |
| La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud por parte de un tercero | 1 | 0,5 | 1 | 1 | | 3,5 | |
| **2.6 Criterios para el tratamiento de datos en relación con aliados comerciales** | | | | | | **4** | |
| La empresa especifica los criterios para decidir con qué aliados comerciales y en qué condiciones comparte datos personales de sus usuarios | 1 | 1 | 1 | 1 | | 4 | |

| DIRECTV | PUBLICIDAD | CLARIDAD | FACILIDAD | ACCESIBILIDAD | LENGUAJE INCLUSIVO (BONIFICACIÓN) | SUMA POR CRITERIO | PROMEDIO POR EJE |
|---|---|---|---|---|---|---|---|
| **3. LIBERTAD DE EXPRESIÓN** | | | | | | | **0** |
| **3.1. Informa sobre la obligación legal de bloqueo** | | | | | | **1** | |
| 3.1.1 Informa si bloquea contenidos por explotación de personas menores de edad, juegos de suerte y azar y órdenes judiciales. | 0,33 | 0,33 | 0,33 | 0,33 | | 1,32 | |
| 3.1.2 Informa el soporte legal | 0,33 | 0,33 | 0,33 | 0,33 | | 1,32 | |
| **3.2 Procedimientos de bloqueo (incluye obligación contractual)** | | | | | | **0** | |
| 3.2.1. Informa el procedimiento que sigue para el bloqueo según los criterios que emplea para filtrar, retirar o bloquear contenidos (legales y contractuales), | 0 | 0 | 0 | 0 | | 0 | |
| 3.2.2 Cuando bloquea por motivos contractuales tiene un procedimiento de queja para los usuarios | 0 | 0 | 0 | 0 | | 0 | |
| 3.2.3 Anuncia a usuarios el motivo del bloqueo | 0 | 0 | 0 | 0 | | 0 | |
| **3.3. Guía sobre comportamientos no permitidos** | | | | | | **0** | |
| La empresa pública en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones | 0 | 0 | 0 | 0 | | 0 | |
| **4. SEGURIDAD DIGITAL** | | | | | | | **2** |
| **4.1. Informa de fuga de datos personales y acciones de mitigación** | | | | | | **0** | |
| 4.1.1 Notificación sin demora indebida a las autoridades pertinentes | 0 | 0 | 0 | 0 | | 0 | |
| 4.1.2 Notificación a las personas afectadas | 0 | 0 | 0 | 0 | | 0 | |
| 4.1.3 El tipo de medidas que la empresa puede tomar para mitigar los daños | 0 | 0 | 0 | 0 | | 0 | |
| **4.2. Uso de protocolo de seguridad (HTTPS) en su sitio web** | | | | | | **4** | |
| | 1 | 1 | 1 | 1 | | 4 | |

# ANEXO

### 1. Ejes temáticos

Como en pasadas ediciones, **¿Dónde están mis datos?** 2019 es un sistema de evaluación que contrasta los compromisos públicos de las empresas proveedoras de internet tanto en el aspecto de políticas corporativas, como en el respeto y la atención que ofrecen a la intimidad, la libertad de expresión y la seguridad digital de las personas que usan sus servicios.
En consecuencia, los ejes que evaluamos son:

**Compromisos políticos.** Entendemos por políticas el "Conjunto de conceptos, decisiones, programas y acciones con sentido deliberado y específico cuyo avance y proceso debe examinarse en forma permanente"[1]. Es decir, las políticas que las empresas adoptan en diferentes temas es la forma como materializan sus compromisos políticos. Son la manera en la que las empresas dan importancia a problemáticas sociales. Nos interesa analizar y promover aquellas con las que estas empresas pueden generar un compromiso hacia la inclusión e igualdad, y una responsabilidad frente a la transparencia de sus operaciones. Inicialmente, la manera en la que medimos esto es considerando que las empresas tengan políticas de género y de accesibilidad para personas con discapacidad, y que publiquen un informe de transparencia (o su equivalente) para Colombia, al menos anualmente.

**Intimidad.** A través de formas concretas, las empresas demuestran el respeto a la intimidad de las personas que contratan sus servicios. La intimidad es un derecho fundamental reconocido en el Artículo 15 de la Constitución Política de Colombia. La evaluación también se concentra en que las empresas adopten políticas de protección y desarrolla insumos para analizar compromisos específicos de esas políticas. Entre otros aspectos damos importancia a  que informen sobre la exigencia legal que tienen de retener datos, las bases legales por las que están obligadas a atender solicitudes de información de datos personales, los procedimientos que usan para entregar esos datos y si notifican a las personas sobre la entrega de su datos a terceros. Vale la pena resaltar que en la evaluación de 2019 se buscó también identificar la información que las empresas dan a conocer sobre los acuerdos que pactan con terceros para compartir nuestros datos.

**Libertad de expresión.** El rol de las empresas proveedoras de internet es clave para el respeto a la libertad de expresión de las personas que contratan sus servicios. Considerando que la libertad de expresión es un derecho fundamental reconocido en el Artículo 20 de la Constitución Política de Colombia, en nuestra evaluación tenemos en cuenta que las empresas realicen un esfuerzo por proteger ese derecho a través de la divulgación de las obligaciones legales que tienen frente a bloqueos de internet y de páginas de internet, y a los procedimientos que siguen para esto. Además, consideramos que la empresa tenga una guía de comportamientos no permitidos que expliquen a las personas usuarias sobre aquellos que deben evitar para no que no les cancelen o bloqueen servicios.

---

1. Atehortúa, A. y Rojas, D.. (2009). Cifras, impacto y perspectivas de la política de consolidación de la seguridad democrática. Balance 2006-2009. Reflexión para la planeación. Colombia: Ediciones Aurora.

Seguridad digital. Las empresas demuestran a través de acciones concretas su compromiso de garantizar la seguridad de sus productos y servicios. Nuestro interés en que la seguridad digital haga parte de la agenda de las empresas, en aras de la protección de la información privada de las personas que acceden a sus servicios de internet, es prioritario. Por ello la evaluación incluye analizar si informan sobre los procedimientos que emplean en caso de sufrir brechas de seguridad y, por otro, evaluamos si utilizan el protocolo seguro de transmisión de datos (HTTPS) en todos sus sitios web y, particularmente, en aquellos en los que existe un intercambio de información (compras, ventas y/o consulta).

## Criterios de evaluación

| DEFINICIÓN DE CRITERIOS | |
|---|---|
| **1. Compromisos políticos** | |
| **1.1. Política de género.** | La empresa publica en su sitio web para Colombia una política comprometida con la promoción de la igualdad de género que, idealmente, incluye acciones concretas en las siguientes áreas: (1) selección y contratación de personal (diversidad sexual y de género); (2) desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos; (3) equilibrio familiar-laboral (e igualdad en beneficios); (4) prevención del acoso sexual; y (5) promoción de imágenes públicas no sexistas. |
| **1.2. Política de accesibilidad.** | La empresa publica en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos (ej. sitio web) y de información de sus servicios para personas con discapacidad. |
| **1.3. Informes de transparencia.** | La empresa publica periódicamente en su sitio web para Colombia un documento (o documentos) donde aparezcan datos agregados sobre: (1) solicitudes de datos del suscriptor (Decreto 1704 y Ley Inteligencia) donde se indica datos como: número de solicitudes, mes/año de solicitud, autoridad que solicita y número de solicitudes atendidas y no atendidas. (2) Bloqueos de URL o sitios web donde indica datos como: Solicitante (autoridad o titular de derechos), Motivo (pornografía, juegos, orden judicial, orden administrativa), Mes/Año de solicitud, Número de solicitudes atendidas y no atendidas y temporalidad del bloqueo: temporal o definitivo. (3) Interceptaciones de líneas telefónicas donde indica datos como: Tipo de servicio (fijo/móvil), Autoridad que solicita la interceptación, Duración de la interceptación, Número de solicitudes atendidas y no atendidas. |

| 2. Intimidad | |
|---|---|
| **2.1. Políticas de protección de datos.** | La empresa (1) publica en el sitio web para Colombia su política de protección de datos, y esa política es específica en indicar (2) qué datos recoge, (3) cuáles son los usos que hace de los datos e (4) indica los terceros que acceden a los datos que recoge. |
| **2.2. Informa la obligación legal de retención de datos.** | La empresa informa públicamente (1) que está obligada por ley a retener datos, (2) el tipo de datos que retiene y (3) el tiempo por el que los retiene. |
| **2.3. Informa las razones para responder a solicitudes de información por parte de entidades públicas.** | La empresa da a conocer las bases legales y las razones por las que está obligada a cumplir con solicitudes de datos personales por parte del sector público. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa. |
| **2.4. Procedimiento de entrega de datos al sector público.** | La empresa da a conocer su procedimiento para responder a solicitudes de información del sector público. Con este propósito ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes y tiene mecanismos que garanticen los derechos de los usuarios (por ejemplo cuenta con un defensor del usuario que analiza estas solicitudes con base en criterios garantistas de derechos humanos). |
| **2.5. Notifica a las personas sobre la entrega de datos a entidades públicas.** | La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud por parte de una autoridad administrativa o judicial. |
| **2.6 Criterios para el tratamiento de datos en relación con aliados comerciales.** | La empresa especifica los criterios para decidir con qué aliados comerciales y en qué condiciones comparte datos personales de sus usuarios. |

| 3. Libertad de expresión | |
|---|---|
| **3.1. Informa sobre la obligación legal de bloqueo.** | La empresa publica en el sitio web para Colombia que (1) está obligada a filtrar, retirar o bloquear contenidos relacionados con la explotación de personas menores de edad, juegos de suerte y azar, órdenes judiciales y estados de excepción. indicando los soportes legales y (2) informa el el soporte legal de estas acciones. |
| **3.2. Procedimientos de bloqueo (incluye obligación contractual).** | La empresa publica en el sitio web para Colombia (1) el el procedimiento que sigue para el bloqueo según los criterios que emplea para filtrar, retirar o bloquear contenidos (legales y contractuales), (2) cuando bloquea por motivos contractuales tiene un procedimiento de queja para las personas usuarias, (3) anuncia a quienes usan internet el motivo del bloqueo. |
| **3.3. Guía sobre comportamientos no permitidos** | La empresa publica en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones. |
| **4. Seguridad digital** | |
| **4.1. Informa de fuga de datos personales y acciones de mitigación.** | La empresa informa públicamente su procedimiento para responder a las brechas de seguridad, incluyendo (1) notificación sin demora indebida a las autoridades pertinentes; (2) notificación a las personas afectadas, y (3) el tipo de medidas que la empresa puede tomar para mitigar los daños. |
| **4.2. Uso de protocolo de seguridad HTTPS en su sitio web.** | La empresa tiene activado de forma predeterminada el protocolo seguro de transmisión de datos (HTTPS) en el sitio web de Colombia. |

## Indicadores de evaluación

### A. Indicadores para la evaluación de criterios basados en documentos

En este examen, empleamos un sistema de indicadores que nos permite medir la forma como las personas usuarias reciben esta información de las empresas proveedoras frente a cada uno de los puntos evaluados, ese puntaje se multiplica por el indicador de información:

**1. Publicidad.** Que la información esté publicada. Entendemos que la información es pública cuando se encuentra en el sitio web de la empresa en Colombia y está disponible en español.

La valoración se hace de la siguiente manera:

- El documento es público en el sitio web de la empresa en Colombia y está disponible en español. (1 punto)
- El documento es público pero no aparece en el sitio web de la empresa en Colombia y/o está en otro idioma. (0,5 puntos)
- El documento no se encuentra disponible en el sitio web de la empresa en Colombia ni está disponible en español. (0 puntos)

**2. Claridad.** Que la información sea presentada en un lenguaje no técnico, comprensible para cualquier persona. Esto quiere decir que la información es comprensible para un público amplio, no especializado, de diferentes edades y en contextos sociales y culturales diversos.

La evaluación de base en relación con la claridad de los documentos la hacen estudiantes universitarios practicantes de Fundación Karisma. Estas personas se aproximan a los documentos como usuarias de internet. Cuando tienen dudas en relación con la claridad de algunos documentos Karisma pide valoración de los mismos a personas externas que representen perfiles no especializados (ni en tecnología ni en derecho) con características diversas en género y en edad.

El valor que se asigna corresponde a la siguiente clasificación:

- El texto está escrito en forma sencilla, es de fácil comprensión, no tiene lenguaje técnico o, teniendo lenguaje técnico, está suficientemente explicado y no genera confusiones. (1 punto)

- El texto está escrito de forma moderadamente compleja, contiene lenguaje técnico que no es suficientemente claro o no está adecuadamente explicado, lo que dificulta su comprensión. (0,5 puntos)
  El texto está escrito en forma muy compleja, contiene mucho lenguaje técnico que no está explicado y no se logra su comprensión. (0 puntos)

**3. Facilidad.** Que la información sea fácil de encontrar en el sitio web de la empresa en Colombia (número de clics). Entendemos que la información es fácil de encontrar cuando se encuentra en el sitio web principal de la empresa y/o tiene un enlace que lleva directamente a esta.

La valoración se hace de la siguiente manera:

- 1 a 2 clics = muy fácil (1 punto)
- 3 a 4 clics = fácil (0,5 puntos)
- 5 o más clics = difícil (0 puntos)

**4. Accesibilidad.** Que el mayor número de personas, incluidas aquellas que tienen algún tipo de discapacidad o dificultad para la lectura, puedan utilizar y acceder a la información.

En la evaluación de este año solamente tuvimos en cuenta que la información esté presentada en un documento navegable, en el que puedan realizarse búsquedas y del que se puedan copiar y pegar partes. Entendemos que esto último aumenta la posibilidad de que la información sea usada efectivamente por más personas para indagar sobre sus derechos y deberes. Además, mejora la probabilidad de que los lectores automáticos la reconozcan para beneficio de personas con dificultad para la lectura.
La valoración se hace de la siguiente manera:

- El documento es navegable, permite búsquedas y se pueden copiar partes del texto. (1 punto)
- El documento es navegable o permite búsquedas o se pueden copiar partes del texto. (0,5 puntos)
- El documento no es navegable, no permite búsquedas ni copiar partes del texto. (0 puntos)

**5. Lenguaje inclusivo.** Este año, nuevamente, no dimos un puntaje al lenguaje inclusivo dentro de la evaluación. Los esfuerzos que las empresas hagan por hacer más incluyentes sus documentos fueron tenidos en cuenta y se bonificaron hasta con un (1) punto. Respecto al lenguaje inclusivo y su importancia en una política de género y contra la discriminación se puede consultar:

- *Guía para el lenguaje incluyente* de la Alcaldía Mayor de Bogotá, Colombia[2].
- *Manuales y textos para el lenguaje incluyente*, recopilados por la Universidad Nacional de Colombia[3].
- *Guía para el lenguaje inclusivo y no discriminatorio* de CETEO en España[4].
- *Guía para la revisión del lenguaje desde una perspectiva de género*, elaborado por la Dra.
- Mercedes Bengoechea de la Universidad de Alcalá de Henares, España[5].

## B. Indicador especial para el criterio técnico de seguridad digital: implementación del protocolo HTTPS

Implementar el protocolo HTTPS es la mínima medida de seguridad digital que deben aplicar los responsables de sitios web. Es una práctica que cada vez más se exige a los administradores de sitios web con el fin de proteger las información de las personas. Sin embargo, en algunos casos, aunque se tiene una versión segura del sitio, se ofrece acceso a una versión insegura de forma predeterminada. Esta es una mala práctica.

2. Alcaldía Mayor de Bogotá. (2015). Guía para el lenguaje incluyente. Bogotá, Colombia: Secretaria Distrital de Hacienda. Disponible en
*http://www.shd.gov.co/shd/sites/default/files/documentos/todo_guia_lenguaje.pdf.*

3. Universidad Nacional de Colombia. (s.f.) Manuales y textos sobre lenguaje incluyente. Disponible en
*http://www.humanas.unal.edu.co/nuevo/titulo-manuales-y-textos-sobre-lenguaje-incluyente/*

4. CETEO. (s.f.) Guía para el lenguaje inclusivo y no discriminatorio. Disponible en
*http://www.aspaymcyl.org/pdf/Memorias/GUIA%20LENGUAJE%20NO%20SEXISTA%20E%20INCLUISVO_CETEO.pdf.*

5. Bengoechea, M. (s.f.). Guía para la revisión del lenguaje desde una perspectiva de género. Disponible en
*http://www.bizkaia.eus/home2/Archivos/DPTO1/Noticias/Pdf/Lenguaje%20Gu%C3%ADa%20lenguaje%20no%20sexista%20castellano.pdf.*

Para que se otorguen cuatro puntos en la evaluación de este criterio, se requiere que la empresa tenga implementado de forma predeterminada el protocolo HTTPS en la totalidad de su sitio web. Es decir, que cuando una persona escribe en su navegador la dirección web de la empresa entra automáticamente a la versión segura del sitio.

- Es posible que, en algunas circunstancias, las personas entren a la versión segura del sitio web a pesar de que la empresa no tienen activada de forma predeterminada la implementación del protocolo HTTPS:

- Ingresando al sitio web de la empresa a través de buscadores que redireccionan a la versión segura del mismo. En esos casos, el mérito es del buscador, no de la empresa. Instalando complementos a los navegadores (ej. HTTPS Everywhere) que despliegan de forma automática la versión segura de los sitios web, a pesar de que no sea la versión predeterminada. Nuevamente, en este caso, el mérito no es de la empresa, sino de la persona.

- Implementación parcial del protocolo HTTPS para algunas páginas del sitio web (ej. páginas donde hay intercambio de información como compras o autenticaciones).

En ninguno de estos casos otorgamos puntaje por no cumplir con los componentes del criterio: implementación del protocolo HTTPS y uso en forma predeterminada. En suma, si no se tiene HTTPS predeterminado en el sitio no se obtiene puntaje.

Ahora bien, excepcionalmente se reconocerá la mitad del puntaje si a pesar de que se encuentra HTTPS implementado por defecto, por situaciones anómalas se encuentra que no es realmente así, como cuando encontramos en la evaluación que los documentos que revisamos no están dentro de esta implementación.

Finalmente, si le interesa ver las tablas con valores más detallados puede consultarlas en su versión digital en:
*https://stats.karisma.org.co/donde-estan-mis-datos-2019/*

El informe ¿Dónde están mis datos? 2019 es la quinta publicación que realiza la Fundación Karisma de esta serie.

Esta investigación busca que las empresas proveedoras de internet ofrezcan más información a las personas que usan sus servicios para que mejoren su capacidad de hacer efectivos sus derechos humanos.

Para conocer y descargar el texto completo de este año visita.
*https://stats.karisma.org.co/donde-estan-mis-datos-2019/*

Puedes conocer los informes anteriores en
*https://karisma.org.co/DEMD/*

# ¿Dónde están mis datos?

Informe 2019



Un informe de:

Fundación Karisma

Con el apoyo de:

ELECTRONIC FRONTIER FOUNDATION